PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-218837
(43)Date of publication of application : 19.08.1997

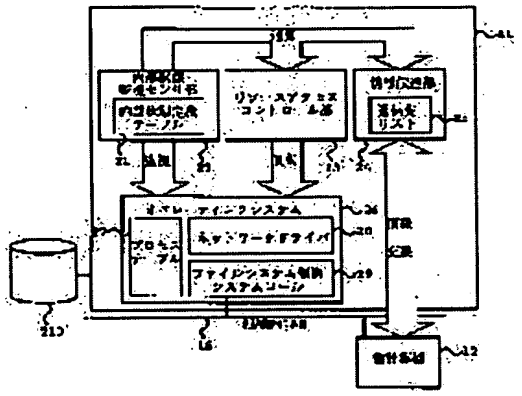
(51)Int.Cl. G06F 13/00
G06F 12/14
H04L 12/24
H04L 12/26

(21)Application number : 08-022780
(22)Date of filing : 08.02.1996

(71)Applicant : HITACHI LTD
(72)Inventor : KAYASHIMA MAKOTO
TERADA MASATOSHI

(54) NETWORK SECURITY SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To realize a dynamic access and to improve the security for an intrusion by performing the protective processing of the internal resource related to an abrnoamlity when the occurrence of the abnormality is detected by an internal state monitoring means.
SOLUTION: An internal state monitoring sensor part 22 monitors an operating system 26. When an abnormality is detected, a resource access control part 23 executes an access control processing for the operating system 26 and an information transmission part 24 notifies the other computer 12 entered in a communication destination list 25 of the detection of the abnormality via a private LAN 16. When the detection of the abnormality is notified to a computer 11 from the other computer 12, the information transmission part 24 notifies the resource access control part 23 of the detection of the abnormality in the other computer after the part 24 confirms whether the other computer 12 of a transmission origin is entered in the communication destination list 25 or not.



LEGAL STATUS

[Date of request for examination]	28.02.2000
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3165366
[Date of registration]	02.03.2001
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－218837

(43)公開日　平成９年(1997)８月19日

(51)Int.Cl.⁶		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	13/00	３５１		Ｇ０６Ｆ	13/00	３５１Ｚ
	12/14	３２０			12/14	３２０Ａ
Ｈ０４Ｌ	12/24		9466－5K	Ｈ０４Ｌ	11/08	
	12/26					

審査請求　未請求　請求項の数11　ＯＬ　（全 14 頁）

(21)出願番号　特願平8－22780

(22)出願日　平成８年(1996)２月８日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　萱島　信
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

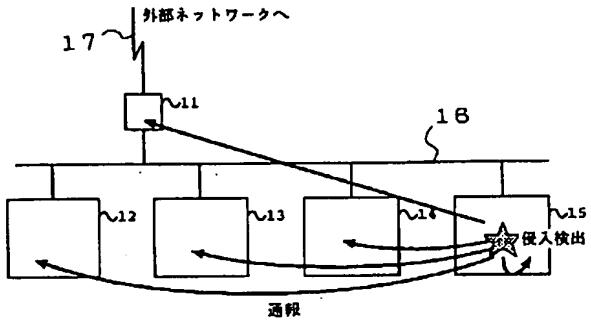
(72)発明者　寺田　真敏
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　富田　和子

(54)【発明の名称】　ネットワークセキュリティシステム

(57)【要約】
【課題】ネットワークに接続された計算機システムにおいて、組織外からの侵入者に対して個々の計算機のセキュリティを強化する。
【解決手段】ファイアウォール内の個々の計算機で、起動しているプロセスの個数、ネットワークインタフェースのトラフィック、特定ファイルのアクセス状況等の内部状態を監視することにより、侵入検出を行ない、異常と判断した場合に、自計算機のリソースアクセスの制御および、ファイアウォールを含む他計算機への侵入の通知を行なう。これにより、自組織内の計算機リソースの保護を行なうことができる。特にファイアウォールに対して侵入検出を通知することにより、自組織全体の計算機リソースの保護を一括して行なうこともできる。

図１



1

【特許請求の範囲】

【請求項１】ネットワークに接続された計算機を有するネットワークセキュリティシステムであって、

前記計算機は、

計算機の内部状態を監視し、異常の発生を検知する内部状態監視手段と、

内部のリソースに対するアクセスの制御を行うアクセス制御手段とを備え、

該アクセス制御手段は、前記内部状態監視手段により異常の発生が検知されたとき、当該異常に関連した内部のリソースの保護処理を行うことを特徴とするネットワークセキュリティシステム。

【請求項２】前記計算機は、前記内部状態監視手段により異常の発生が検出されたとき、前記ネットワークに接続された他の計算機へその旨通知するとともに、前記他の計算機からの異常の発生の通知を受信する情報伝達手段を備え、前記アクセス制御手段は、他の計算機からの異常の発生の通知を受信したときも当該異常に関連した内部のリソースの保護処理を行うことを特徴とする請求項１記載のネットワークセキュリティシステム。

【請求項３】外部ネットワークに接続された内部ネットワークにおいて、該内部ネットワークに接続された計算機において、該計算機の内部状態の監視処理を行ない、該監視処理により前記外部ネットワークからの侵入を検出すると、アクセス制御による計算機リソースの保護処理と、前記内部ネットワークの他の計算機への検出内容の通知処理とを行なうことを特徴とするネットワークセキュリティシステム。

【請求項４】前記内部ネットワークに接続された計算機は、前記内部ネットワーク内の他の計算機からの通知待ち処理を行ない、前記外部ネットワークからの侵入の通知を受けると、アクセス制御による計算機リソースの保護処理を行なうことを特徴とする請求項３記載のネットワークセキュリティシステム。

【請求項５】ネットワークに接続した計算機において、計算機の内部状態の監視処理および、周囲の計算機からの通知待ち処理を行ない、前記ネットワーク外部からの侵入を検出すると、前記ネットワーク内の周囲の計算機とお互いに通知し合うことにより、連係して侵入対策を行なうことを特徴とするネットワークセキュリティシステム。

【請求項６】前記計算機は、実行プロセスの数と、ネットワークインタフェースのトラフィックと、重要なファイルへのアクセスの少なくとも１つを監視し、該監視の結果が、予め定めた制限内容から外れる場合に、異常が発生したと判断する請求項１～５のいずれかに記載のネットワークセキュリティシステム。

【請求項７】前記計算機において、監視による異常の検出状況に応じて、段階的にアクセス制御を実施することにより計算機リソースの保護を行なうことを特徴とする

2

請求項１～６のいずれかに記載のネットワークセキュリティシステム。

【請求項８】前記計算機において、監視の結果得られたデータと、あらかじめテーブルに登録しておいた計算機の内部状態データとを比較することにより、前記異常として外部からの侵入を判定することを特徴とする請求項１～７のいずれかに記載のネットワークセキュリティシステム。

【請求項９】前記テーブルの内容をユーザが決定することを特徴とする請求項８記載のネットワークセキュリティシステム。

【請求項１０】前記計算機において、前記テーブルの内容の更新時に、他の計算機に上記テーブルの内容を通知し、他の計算機は上記通知内容に基づき、自己のテーブルの内容を更新することを特徴とする請求項９記載のネットワークセキュリティシステム。

【請求項１１】ネットワークに接続した計算機において、複数のサーバが連動することにより動作するサービスが稼働しているネットワークシステムに対して、連係して侵入対策を行なうと共に、侵入対策に応じて連動サービスの動作を変更することを特徴とする請求項２記載のネットワークセキュリティシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークに接続した計算機のセキュリティに係わり、特に計算機とファイアウォールが連係して組織外からの侵入者に対する防御を実行するネットワークセキュリティシステムに関する。

【０００２】

【従来の技術】従来、ネットワークを経由した計算機への侵入に対する防御策として、外部とのアクセスに制限を施すファイアウォール（ｆｉｒｅｗａｌｌ）が提案されている。ファイアウォールは、送信元と送信先のＩＰアドレスの組合せによりアクセス制御を施すもので、（１）サービス毎にリソースにアクセスできるＩＰアドレスを制限し、（２）アクセス記録を残す機能を持つものが主流である。このなかで、チェックポイント（Ｃｈｅｃｋｐｏｉｎｔ）社の製品であるＦｉｒｅｗａｌｌ－１は、ゲートウェイだけでなく、各計算機もそれぞれアクセス制御を行なう機能を持ち、各計算機の設定は１台の計算機で管理できるようになっている。

【０００３】

【発明が解決しようとする課題】インターネットの発展により、世界中で発信している情報を手元の計算機でリアルタイムに入手できるようになった反面、自計算機も外部からの侵入者の脅威にさらされることになった。このような侵入者に対する防御策として、（１）サービス毎にリソースにアクセスできるＩＰアドレスを制限し、（２）アクセス記録を残す、ゲートウェイ（狭義のファ

イアウォール）が提案されている。狭義のファイアウォールを使用することにより、管理者が監視する範囲を限定することができる。しかし、個々の計算機は逆にチェックが甘くなるため、万が一ファイアウォールをすり抜けて侵入されると、その侵入された計算機を足掛かりにして周囲の計算機に攻撃を仕掛けられる可能性がある。前述したＣｈｅｃｋｐｏｉｎｔ社のＦｉｒｅｗａｌｌは、狭義のファイアウォール以外に、（１）サービス毎にリソースにアクセスできるＩＰアドレスの制限を各計算機単位で行ない、（２）アドレス制限の設定はリモートで実施することにより、１台の計算機でその設定作業を行なうことができる、という特徴を持っている。しかし、アクセス制御の設定は静的に定義するものであり、一度侵入された場合には管理者がファイアウォールと各計算機に対して対策を施す必要があった。

【０００４】そこで本発明では、（１）ファイアウォール内の個々の計算機で侵入の検出を行ない、（２）その結果を周囲にフィードバックする仕組みを提供することにより、動的なアクセスを実現し、侵入に対するセキュリティを高めることを目的とする。

【０００５】

【課題を解決するための手段】上記課題を解決するために、本発明は、ネットワークに接続された計算機を有するネットワークセキュリティシステムであって、前記計算機は、計算機の内部状態を監視し、異常の発生を検知する内部状態監視手段と、内部のリソースに対するアクセスの制御を行うアクセス制御手段とを備え、該アクセス制御手段は、前記内部状態監視手段により異常の発生が検知されたとき、当該異常に関連した内部のリソースの保護処理を行うことを特徴とするネットワークセキュリティシステムを提供する。

【０００６】前記計算機は、好ましくは、前記内部状態監視手段により異常の発生が検出されたとき、前記ネットワークに接続された他の計算機へその旨通知するとともに、前記他の計算機からの異常の発生の通知を受信する情報伝達手段を備え、前記アクセス制御手段は、他の計算機からの異常の発生の通知を受信したときも当該異常に関連した内部のリソースの保護処理を行う。

【０００７】本発明は、他の見地によれば、外部ネットワークに接続された内部ネットワークにおいて、該内部ネットワークに接続された計算機において、該計算機の内部状態の監視処理を行ない、該監視処理により前記外部ネットワークからの侵入を検出すると、アクセス制御による計算機リソースの保護処理と、前記内部ネットワークの他の計算機への検出内容の通知処理とを行なうことを特徴とするネットワークセキュリティシステムを提供する。

【０００８】前記内部ネットワークに接続された計算機は、好ましくは、前記内部ネットワーク内の他の計算機からの通知待ち処理を行ない、前記外部ネットワークからの侵入の通知を受けると、アクセス制御による計算機リソースの保護処理を行なう。

【０００９】本発明は、さらに他の見地によれば、ネットワークに接続した計算機において、計算機の内部状態の監視処理および、周囲の計算機からの通知待ち処理を行ない、前記ネットワーク外部からの侵入を検出すると、前記ネットワーク内の周囲の計算機とお互いに通知し合うことにより、連係して侵入対策を行なうことを特徴とするネットワークセキュリティシステムを提供する。

【００１０】前記計算機は、実行プロセスの数と、ネットワークインタフェースのトラフィックと、重要なファイルへのアクセスの少なくとも１つを監視し、該監視の結果が、予め定めた制限内容から外れる場合に、異常が発生したと判断することができる。

【００１１】前記計算機において、監視による異常の検出状況に応じて、段階的にアクセス制御を実施することにより計算機リソースの保護を行なうことも可能である。

【００１２】前記計算機において、監視の結果得られたデータと、あらかじめテーブルに登録しておいた計算機の内部状態データとを比較することにより、前記異常として外部からの侵入を判定することができる。このテーブルの内容は、ユーザが決定することができる。

【００１３】前記計算機において、前記テーブルの内容の更新時に、他の計算機に上記テーブルの内容を通知し、他の計算機は上記通知内容に基づき、自己のテーブルの内容を更新するようにしてもよい。

【００１４】また、ネットワークに接続した計算機において、複数のサーバが連動することにより動作するサービスが稼働しているネットワークシステムに対して、連係して侵入対策を行なうと共に、侵入対策に応じて連動サービスの動作を変更することも可能である。

【００１５】本発明のネットワークセキュリティシステムでは、組織内の個々の計算機がそれぞれ侵入を検出する処理と、侵入を検出した場合に計算機リソースの保護処理および、周囲の他計算機に対する通知処理を行なうことにより、外部からの侵入に対してセキュリティを強化すると共に、管理者に対して侵入を早期に伝達することができる。

【００１６】

【発明の実施の形態】本発明の一実施の形態を、図１から図１０を用いて説明する。図１は、本発明を適用したネットワークセキュリティシステムの全体構成を示す図である。１１はファイアウォールとしての計算機、１２から１５は組織内ＬＡＮ１６に接続された計算機、１７はファイアウォール１１と外部ネットワークとの接続を行なう専用線である。例えば、計算機１５において、外部からの不当な侵入を検出した場合には、後述するようなアクセスコントロール制御処理を自計算機において実

5

行するとともに、組織内ＬＡＮ１６に接続された他の計算機１１、１２～１４へ不当な侵入の発生を通知する。この通知を受けた計算機においても、アクセスコントロール制御処理を行う。

【００１７】図２は、図１のネットワークセキュリティシステムで使用する計算機１１の概要を示す図である。２１は内部状態定義テーブル、２２は内部状態監視センサ部、２３はリソースアクセスコントロール部、２４は情報伝達部、２５は通知先一覧リスト、２６はオペレーティングシステム、２７はプロセステーブル、２８はネットワークドライバ、２９はファイルシステム制御システムコール、２１０は外部記憶装置である。

【００１８】内部状態監視センサ部２２は、オペレーティングシステム２６を監視し、監視結果を内部状態定義テーブル２１の内容と比較することにより侵入を検出する。内部状態監視センサ部２２で異常が検出されると、リソースアクセスコントロール部２３および情報伝達部２４に通知され、リソースアクセスコントロール部２３はオペレーティングシステム２６に対してアクセスコントロール制御処理を実行し、情報伝達部２４は通信先リスト２５に記載されている他計算機１２に対して異常を検出したことを組織内ＬＡＮ１６を経由して通知する処理を実行する。アクセスコントロール処理の内容については後述する。また、他計算機１２から異常を検出したことが計算機１１に通知されてきたた場合、情報伝達部２４は送信元の他計算機１２が通信先一覧リスト２５に記載されているか確認した後、リソースアクセスコントロール部２３に他計算機での異常の検出を通知し、リソースアクセスコントロール部２３はオペレーティングシステム２６に対してアクセスコントロール処理および、実行中のジョブに対する制御を実行する。「実行中のジョブに対する制御」は、例えばＵＮＩＸシステムの場合、管理者の権限で実行中のプロセスを終了させることや、プロセスの優先度を変更することに相当する。具体的には、計算機の負荷を異常に重くするジョブを実行しているユーザのプロセスを終了、もしくはその優先度を下げることにより、他のサービスを続行することが可能になる。

【００１９】次に、図２の計算機１１で用いられるテーブルおよび送信メッセージの構成について図８、図９、および図１１により説明する。

【００２０】図８は計算機１１の内部状態定義テーブル２１の構造の一例を示した図である。８１はプロセス数定義テーブルであり、計算機１１のユーザＩＤを記述するユーザＩＤフィールド８２と、各ユーザ毎のプロセス数制限値を記述するプロセス数制限値フィールド８３により構成されるレコードの集まりである。８４はパケット数定義テーブルであり、計算機１１と通信可能なネットワークもしくはホストのアドレスを記述するネットワークアドレスフィールド８５と、各ネットワークもしくはホスト毎のトラフィックの制限値を記述するトラフィック制限値フィールド８６により構成されるレコードの集まりである。８７はオープンファイル情報テーブルであり、計算機１１の外部記憶装置２１０に格納されたファイル名を記述するファイル名フィールド８８と、これらのファイルにアクセス可能なユーザのＩＤを記述するアクセスユーザフィールド８９と、前記アクセスユーザがファイルにアクセスする際に使用するプログラムの名称を記述するプログラム名フィールド８１０により構成されるレコードの集まりである。内部状態定義テーブル２１の設定内容は、ユーザが決定することができる。

【００２１】外部からの侵入が発生したとき、ネットワークからのアクセスに対処するサービスを実現するプロセスに対して、（１）想定している以上の個数のプロセスが起動されたり、（２）プロセスが想定している以上の個数のパケットを受信したりする。また、特定のファイルシステムが想定外の利用者からアクセスされる場合がある。図８のテーブルの内容は、これらの事項をチェックすることにより、外部からの侵入を検出するためのものである。

【００２２】図９は内部状態監視センサ部２２からリソースアクセスコントロール部２３および情報伝達部２４に対して送信されるメッセージの構成例を示した図である。この例では、メッセージ９１は、異常の種別を格納するフィールド９２と、内部状態テーブルレコードデータを格納するフィールド９３とを有する。フィールド９２には、「プロセステーブル監視結果」、「ネットワークインタフェース監視結果」、「オープンファイル監視結果」のいずれかが格納される。フィールド９３に格納される内部状態テーブルレコードデータは、プロセス数定義テーブル８１、パケット数定義テーブル８４、オープンファイル情報テーブル８７のレコードのいずれかである。

【００２３】図１１に、プロセステーブル２７の構成例を示す。これは、オペレーティングシステム２６のカーネル内に常駐するテーブルであり、１レコードで１つのプロセスについての情報を保持する。このテーブル２７は、使用情報２７１、スケジューリング情報２７２、資源利用状況に関する情報２７３、他プロセスへのポインタ２７４、テキスト構造体へのポインタ２７５、およびページテーブルへのポインタ２７の各フィールドを有する。使用情報２７１は、個々のエントリ２７８が使用中か否かを示す情報であり、使用中の場合、そのプロセスの実行者（ユーザＩＤ）を示す。スケジューリング情報２７２は、そのプロセスが、「生成」、「実行中」、「待ち」、「実行可」のどの状態にあるかを示す情報である。資源利用状況に関する情報２７３は、そのプロセスが計算機の各入出力デバイスに対し、「使用中」、「待ち」、「その他」のどの状態にあるかを示す情報である。他プロセスへのポインタ２７４は、プロセスを実

6

7

行するために必要な他のプロセス（親プロセス、その他）を指し示すポインタである。テキスト構造体へのポインタ２７５は、他プロセスと共有可能なテキスト領域を指し示すポインタである。ページテーブルへのポインタ２７６は、仮想アドレスと実メモリとの対応関係を保持するテーブルのエントリを指し示すポインタである。本発明では、プロセステーブル２７のエントリ数、および各エントリの使用情報２７１を利用することにより、各ユーザの使用プロセス数を把握する。また、「資源利用状況に関する情報２７３を利用することにより、例えば特定のデバイスへのアクセスを要求しているプロセス数を把握する。

【００２４】図３は、図２に示した計算機において実行される、内部の監視による異常の検出および異常検出時の処理のフローチャートである。まず、内部状態監視センサ部２１が監視データをオペレーティングシステム２６から収集する（ステップ３１）。ついで、取得した監視データを内部状態定義テーブル２１のエントリと比較する（ステップ３２）。ステップ３２で比較した結果、異常があったかどうか判断する（ステップ３３）。異常がなければ、最初のステップ３１へ戻る。異常ありと判定された場合には、内部状態監視センサ部２２よりリソースアクセスコントロール部２３に異常の発生を通知する（ステップ３４）。ステップ３４の通知結果に基づきリソースアクセスコントロール部２３がアクセスコントロール処理を実行する（ステップ３５）。内部状態監視センサ部２２は、また、情報伝達部２４に異常の発生を通知する（ステップ３６）。この通知を受けて、情報伝達部２４は通信先一覧リスト２５より異常の発生を知らせるメッセージの通知先の他計算機を特定する（ステップ３７）。そこで、情報伝達部２４が他計算機１２～１５およびファイアウォール１１に対して異常の発生を知らせるメッセージを送信する（ステップ３８）。

【００２５】図４は、図２に示した計算機において、他計算機が異常を検出したことに応答して行われる異常通知メッセージ受信時の処理のフローチャートである。情報伝達部２４で他計算機からの異常を通知するメッセージを受信する（ステップ４１）。このステップ４１で受信したメッセージが正当な発信者により発信されたものか確認する（ステップ４２）。不当と判断されれば、以後のステップを実行することなく本処理を終了する。正当と判断された場合、情報伝達部２４よりリソースアクセスコントロール部２３に他計算機で発生した異常を通知する（ステップ４３）。この通知結果に基づき、リソースアクセスコントロール部２３がアクセスコントロール処理および、実行中のジョブに対する制御を実行する（ステップ４４）。本処理は特にファイアウォール１１において実行することにより、計算機１２～１５に対するアクセスコントロール処理を一括して実行することができる。

8

【００２６】図５は、内部状態監視センサ部２２において、計算機１１で実行中のプロセスの個数に着目した監視処理の一例を示すフローチャートである。まず、オペレーティングシステム２６内のプロセステーブル２７よりユーザＩＤごとに実行中のプロセス数を取得する（ステップ５１）。次に、このステップで取得したユーザＩＤごとの実行プロセス数を、内部状態定義テーブル２１に記述された当該ユーザＩＤのプロセス数の制限値と比較する（ステップ５２）。いずれのユーザＩＤについても実行中プロセス数がその制限値を越えなければ、一定時間スリープする（ステップ５３）。制限値を越えていた場合には、他の処理部および他の計算機へ通知するメッセージを組み立てる（ステップ５４）。ついで、リソースアクセスコントロール部２３にステップ５４で作成したメッセージを送信する（ステップ５５）。さらに、情報伝達部２４にステップ５４で作成したメッセージを送信する（ステップ５６）。その後、ステップ５１へ戻る。

【００２７】図６は、内部状態監視センサ部２２において、計算機１１のネットワークインタフェース部のトラフィックに着目した監視処理を示すフローチャートである。まず、ネットワークアドレス毎に、オペレーティングシステムのネットワークドライバ２８より単位時間あたりのパケット送受信数を取得する（ステップ６１）。ついで、このステップ６１で取得したパケット数を、ネットワークアドレス毎に、内部状態定義テーブル２１に記述されたパケット数の制限値と比較する（ステップ６２）。いずれのネットワークアドレスについても、制限値を越えていない場合には、一定時間スリープした後（ステップ６３）、最初のステップ６１へ戻る。いずれかのネットワークアドレスについて制限値を越えていた場合には、他の処理部および他の計算機へ通知するメッセージを組み立てる（ステップ６４）。このステップ６４で作成したメッセージをリソースアクセスコントロール部２３に送信する（ステップ６５）。さらに、情報伝達部２４にもこのメッセージを送信する（ステップ６６）。その後、ステップ６１へ戻る。

【００２８】図７は、内部状態監視センサ部２２において、計算機１１のローカルなファイルシステムに対して、ユーザプロセスで当該ファイルシステムへのアクセス要求が発生した時の監視処理を示すフローチャートである。まず、オペレーティングシステム２６からのファイルシステムへのアクセス要求の発生の通知を待つ（ステップ７１）。通知があれば、ファイルシステム制御システムコール２９から、ファイルアクセスを要求したプロセスのＩＤおよび、アクセスされたファイルのＩＤが内部状態監視センサ部２２に通知される。そこで、内部状態テーブル２１のオープンファイル情報テーブル８７を参照することにより、アクセスされたファイルが監視対象かどうか確認する（ステップ７２）。監視対象でな

9

ければ、ステップ７１へ戻る。監視対象であれば、ステップ７１で取得したプロセスＩＤから利用者名および起動プログラム名称を割り出す（ステップ７３）。このステップ７３で割り出した利用者および起動プログラムが、内部状態定義テーブル２１のオープンファイル情報テーブル８７に記載されているものと一致するか（登録されているか）否かを確認する（ステップ７４）。一致していれば、問題ないと判断して、最初のステップ７１へ戻る。一致していなければ、他の処理部および他の計算機へ通知するメッセージを組み立てる（ステップ７５）。ステップ７５で作成したメッセージをリソースアクセスコントロール部２３に送信する（ステップ７６）。さらに、このメッセージを情報伝達部２４に送信する（ステップ７７）。その後、ステップ７１へ戻る。

【００２９】本方式のネットワークセキュリティシステムでは、計算機１１の内部状態の監視処理を、図５から図７までの処理を組み合わせて行なう。

【００３０】図１０は、リソースアクセスコントロール部２３において、内部状態監視センサ部２２から通知（メッセージ）を受信した時の処理を示すフローチャートである。まず、メッセージ９１を受信する（ステップ１０１）。ついで、この受信したメッセージの異常種別９２が「プロセステーブル監視結果」であるか否かを判定する（ステップ１０２）。そうでなければ、異常種別９２が「ネットワークインタフェース監視結果」であるか否かを判定する（ステップ１０３）。ステップ１０２において異常種別９２が「プロセステーブル監視結果」であると判定された場合、内部情報テーブルレコード格納フィールド９３より当該異常と判定されたユーザのユーザＩＤを取得する（ステップ１０４）。ついて、当該ユーザのプロセスの起動制限をオペレーティングシステムに要求する（ステップ１０５）。例えば、オペレーティングシステム２６は、ステップ１０４で取得したユーザＩＤを記憶する領域を持ち、新規プロセス生成時にその記憶領域と照合することにより、当該ユーザについては新たなプロセス生成を抑止する。ステップ１０３において、異常種別９２が「ネットワークインタフェース監視結果」であると判定された場合、メッセージ９１の内部情報テーブルレコード格納フィールド９３より当該異常と判定されたネットワークアドレスを取得する（ステップ１０６）。そこで、当該ネットワークアドレスからのアクセスを遮断するようネットワークインタフェースの設定を変更する（ステップ１０７）。例えば、オペレーティングシステムは、ネットワークインタフェースの入出力に対して、相手先アドレスによるフィルタリングの機能をもち、当該ネットワークアドレスからの通信については入出力を抑止するようネットワークインタフェースの設定を変更する。ステップ１０３において、異常種別９２が「ネットワークインタフェース監視結果」ではないと判定された場合は、メッセージ９１の内部情報

10

テーブルレコード格納フィールド９３よりファイル名を取得する（ステップ１０９）。そこで、このファイルのアクセスパーミッションを変更するようオペレーティングシステムに要求する（ステップ１０９）。オペレーティングシステムは、管理リソースに対するアクセス制御機能を有しており、例えばＵＮＩＸシステムの場合、個々のファイル単位でファイルのオーナであるユーザ、オーナの属するグループのユーザ、その他のユーザの３つのカテゴリに対して「読みとり」、「書き込み」、「実行」の権限を設定することができる。ここでは、グループもしくはその他のユーザに対する「読みとり」権限があったファイルをオーナのみ読みとれるようにする変更、あるいは「書き込み」権限をすべて外すような変更を行う。監視による侵入の検出状況に応じて、段階的にアクセス制御を実施することも可能である。

【００３１】以上、本発明の好適な実施の形態について説明したが、種々の変形・変更を行うことが可能である。例えば、ネットワークに接続した計算機において、監視の対象となるリソースを登録するテーブルの内容の更新時に、他の計算機にそのテーブルの内容を通知し、他の計算機は当該通知内容に基づき、自己の監視の対象となるリソースを登録するテーブルの内容を更新するような構成も可能である。

【００３２】また、ネットワークに接続した計算機において、複数のサーバが連動することにより動作するサービス、例えばネットワークニュースやメールシステムが稼働しているネットワークシステムに対して、連係して侵入対策を行なうと共に、侵入対策に応じて連動サービスの動作を変更することも可能である。具体的には、ネットワークニュースのシステムは、ユーザが最寄りのニュースサーバに対して送信したニュース記事を、隣接するニュースサーバとの間で定期的に交換することにより、すべてのニュースサーバが同一のニュース記事をすべて保持するシステムである。このようなシステムでは、（１）１台のサーバで検出した異常を、ニュースシステムを利用することにより隣接するサーバに対して通知することができ、（２）異常を検出したサーバをシステム全体から分離し、残りのニュースサーバによりニュースシステムのサービスを続行するように設定を変更することが可能となる。

【００３３】

【発明の効果】本発明によれば、ネットワークに接続した計算機において、ネットワークを経由した外部からの侵入に対して自計算機のアクセス制御を行うことと、周囲の計算機へ侵入検出を通知することにより、自組織内の計算機リソースの保護を行なうことができる。特にファイアウォールに対して侵入検出を通知することにより、自組織全体の計算機リソースの保護を一括して行なうこともできる。

【図面の簡単な説明】

11

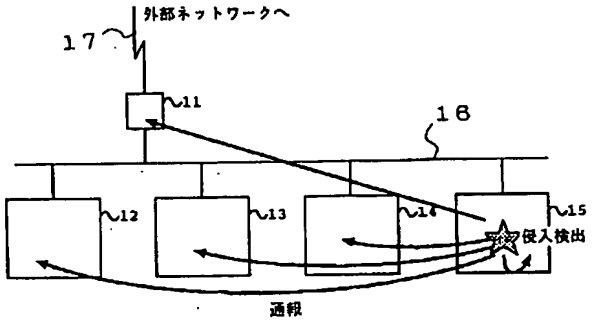
【図１】本発明が適用されるネットワークシステムの全体構成を示すブロック図。
【図２】図１のシステムを構成する計算機の構成例を示すブロック図。
【図３】図２の計算機における内部監視による異常発見時処理のフローチャート。
【図４】図２の計算機における異常通知メッセージ受信時処理のフローチャート。
【図５】図２の計算機におけるプロセステーブル監視処理のフローチャート。
【図６】図２の計算機におけるネットワークトラフィック監視処理のフローチャート。
【図７】図２の計算機におけるファイルシステム監視処理のフローチャート。
【図８】図２の計算機における内部状態定義テーブルの構成例の説明図。
【図９】計算機内の処理部間または計算機間で通信されるメッセージの構成例の説明図。
【図１０】図２の計算機におけるリソースアクセスコントロール部処理のフローチャート。
【図１１】図２の計算機におけるプロセステーブルの構成例の説明図。
【符号の説明】
１１…ファイアウォール、１２～１５…計算機、１６…組織内ＬＡＮ、１７…専用線、２１…内部状態定義テーブル、２２…内部状態監視センサ部、２３…リソースアクセスコントロール部、２４…情報伝達部、２５…通信先一覧リスト、２６…オペレーティングシステム、２７…プロセステーブル、２８…ネットワークドライバ、２９…ファイルシステム制御システムコール、２１０…外部記憶装置、３１…監視データ収集処理、３２…監視データ比較処理、３３…異常判断処理、３４…リソースアクセスコントロール部に対する異常通知処理、３５…リソースアクセスコントロール処理、３６…情報伝達部に

12

対する異常通知処理、３７…通信相手先の特定処理、３８…他計算機に対する異常通知処理、４１…他計算機からの異常通知受信処理、４２…受信メッセージの確認処理、４３…リソースアクセスコントロール部に対する異常通知処理、４４…リソースアクセスコントロール処理、５１…プロセス数取得処理、５２…プロセス数比較処理、５３…スリープ処理、５４…通知メッセージ組み立て処理、５５…リソースアクセスコントロール部に対する送信処理、５６…情報伝達部に対する送信処理、６１…送受信パケット数取得処理、６２…パケット数比較処理、６３…スリープ処理、６４…通知メッセージ組み立て処理、６５…リソースアクセスコントロール部に対する送信処理、６６…情報伝達部に対する送信処理、７１…オペレーティングシステムからの通知待ち処理、７２…アクセスされたファイルが監視対象か確認する処理、７３…利用者名、プログラム名割り出し処理、７４…利用社名、プログラム名が登録されているか確認する処理、７５…通知メッセージ組み立て処理、７６…リソースアクセスコントロール部に対する送信処理、７７…情報伝達部に対する送信処理、８１…プロセス数定義テーブル、８２…ユーザＩＤフィールド、８３…プロセス数制限値フィールド、８４…パケット数定義テーブル、８５…ネットワークアドレスフィールド、８６…トラフィック制限値フィールド、８７…オープンファイル情報テーブル、８８…ファイル名フィールド、８９…アクセスユーザフィールド、８１０…プログラム名フィールド、９１…メッセージ、９２…異常種別格納フィールド、９３…内部状態テーブルレコードデータ格納フィールド、１０１…メッセージ受信処理、１０２…異常種別判定処理、１０３…異常種別判定処理、１０４…ユーザＩＤ取得処理、１０５…プロセス起動制限要求処理、１０６…ネットワークアドレス取得処理、１０７…ネットワーク経由アクセス遮断処理、１０８…ファイル名取得処理、１０９…アクセスパーミッション変更要求処理。

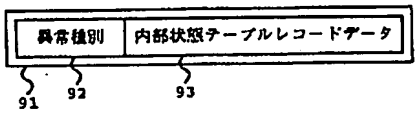
【図１】

図 1



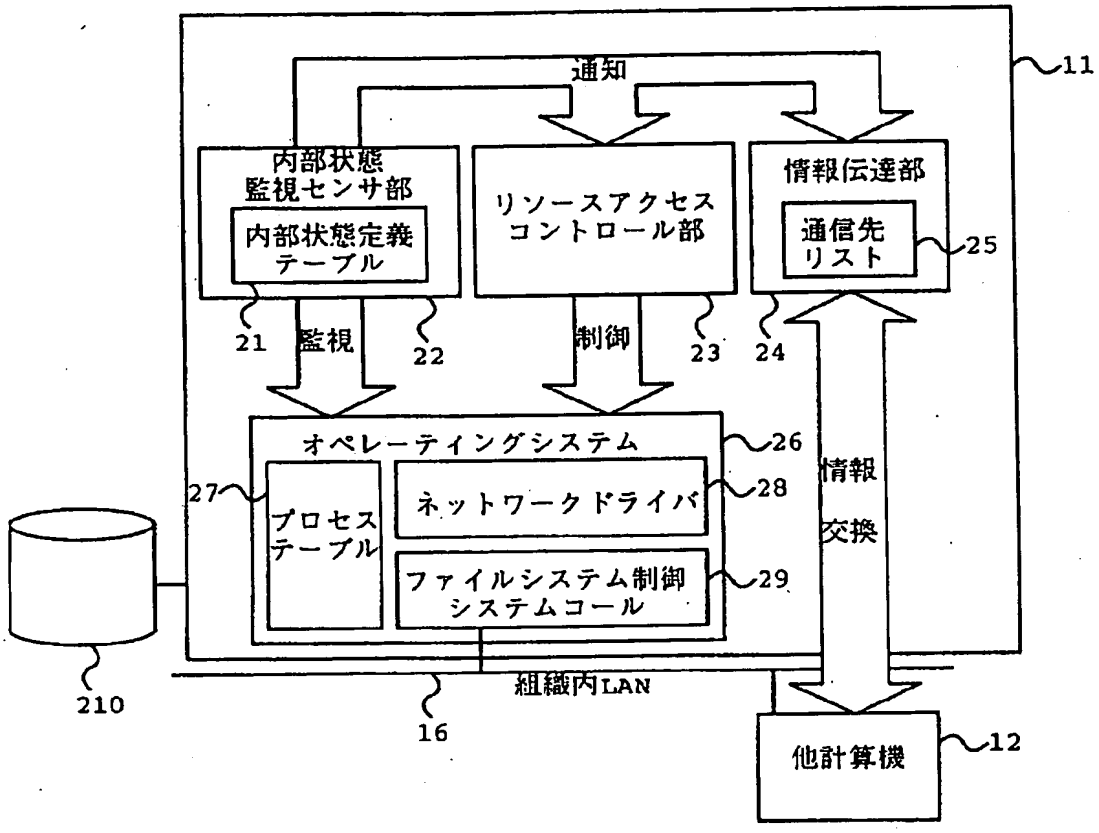
【図９】

図 9



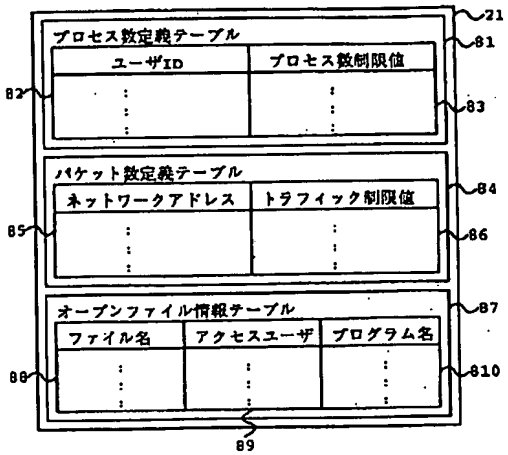
【図２】

図２


11
通知
内部状態
監視センサ部
内部状態定義
テーブル
リソースアクセス
コントロール部
情報伝達部
通信先
リスト
25
21
監視
22
制御
23
24
オペレーティングシステム
26
27
プロセス
テーブル
ネットワークドライバ
28
ファイルシステム制御
システムコール
29
情報
交換
210
組織内LAN
16
他計算機
12

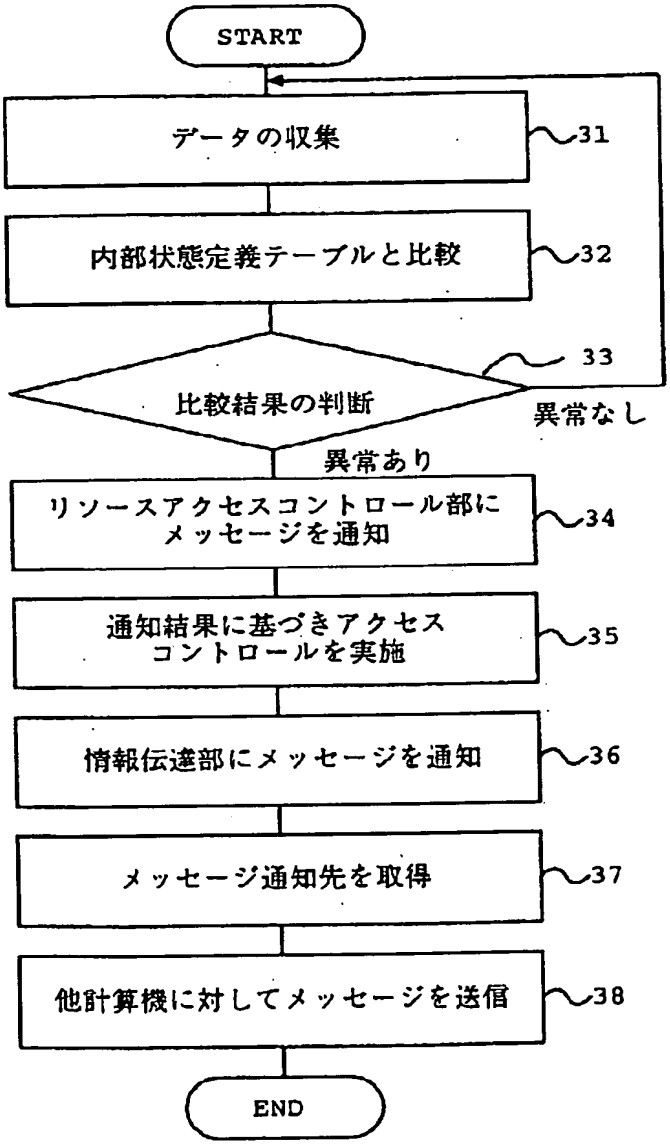
【図８】

図８


21
プロセス数定義テーブル
81
ユーザID
プロセス数制限値
82
83
パケット数定義テーブル
84
ネットワークアドレス
トラフィック制限値
85
86
オープンファイル情報テーブル
87
ファイル名
アクセスユーザ
プログラム名
88
810
89

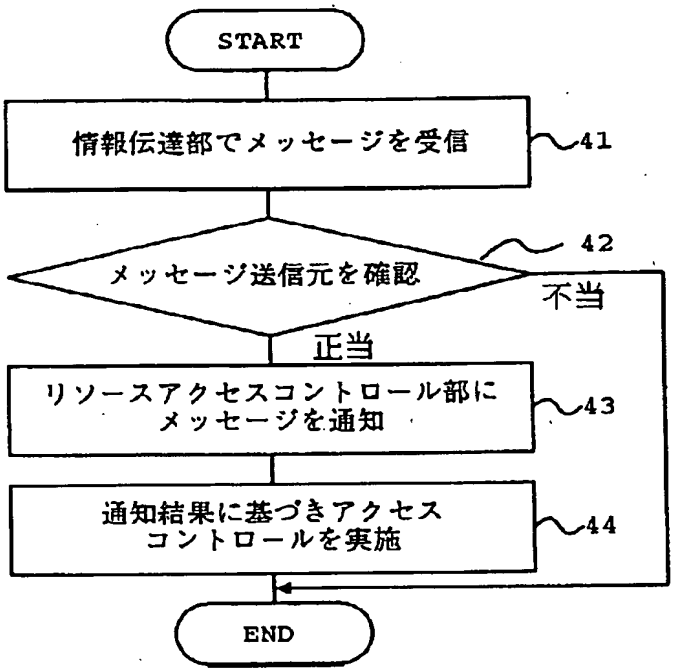
【図３】

図 3


START
データの収集
31
内部状態定義テーブルと比較
32
比較結果の判断
33
異常なし
異常あり
リソースアクセスコントロール部に
メッセージを通知
34
通知結果に基づきアクセス
コントロールを実施
35
情報伝達部にメッセージを通知
36
メッセージ通知先を取得
37
他計算機に対してメッセージを送信
38
END

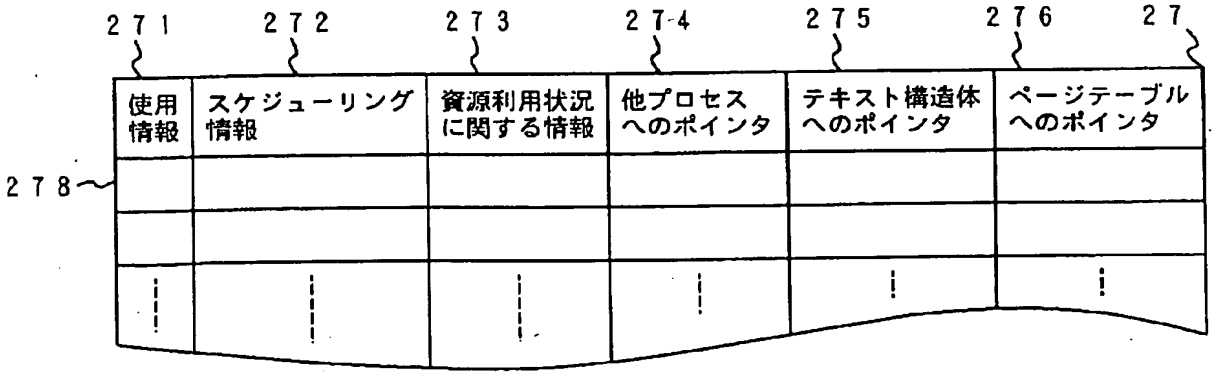
【図4】

図 4


START
情報伝達部でメッセージを受信
41
メッセージ送信元を確認
42
不当
正当
リソースアクセスコントロール部に
メッセージを通知
43
通知結果に基づきアクセス
コントロールを実施
44
END

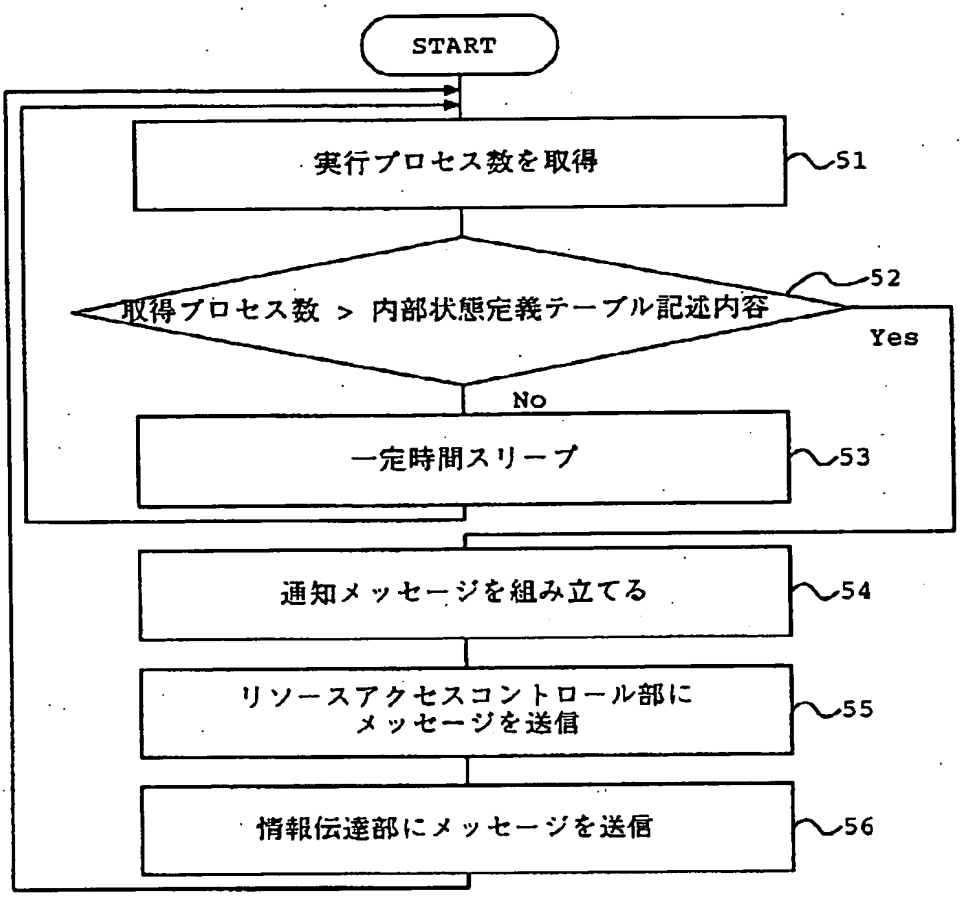
【図11】

図11


271
272
273
274
275
276
27
使用情報
スケジューリング情報
資源利用状況に関する情報
他プロセスへのポインタ
テキスト構造体へのポインタ
ページテーブルへのポインタ
278

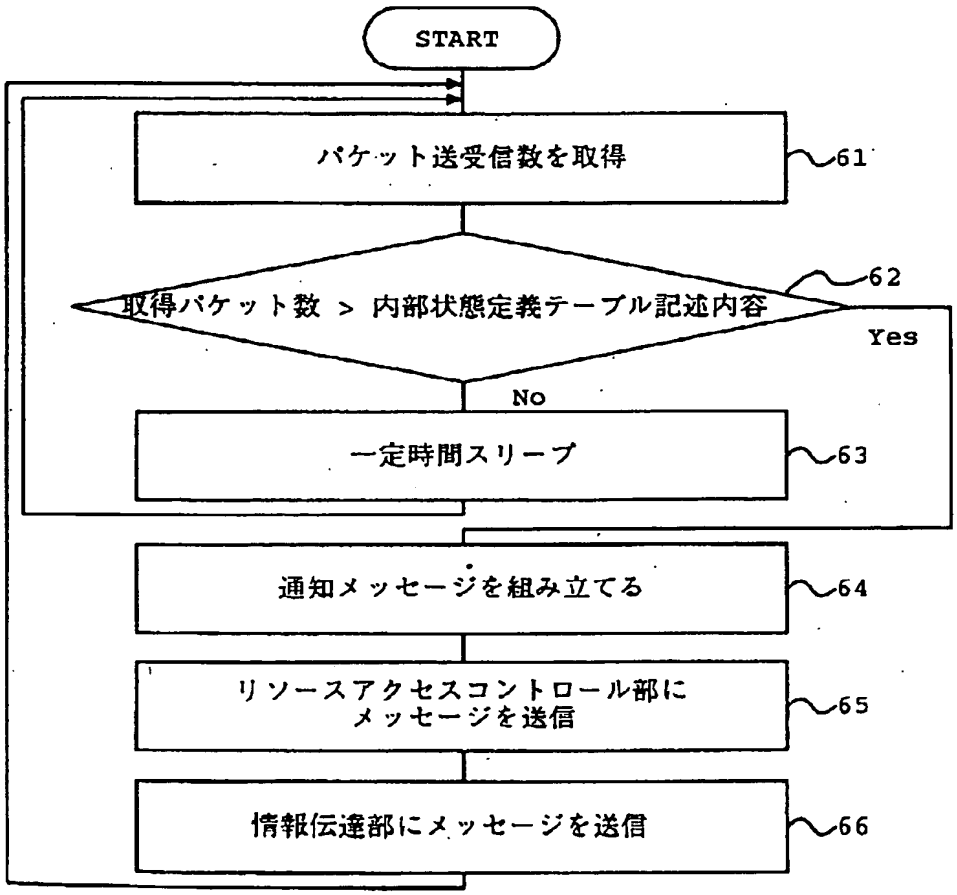
【図5】

図 5


START
実行プロセス数を取得
51
取得プロセス数 > 内部状態定義テーブル記述内容
52
Yes
No
一定時間スリープ
53
通知メッセージを組み立てる
54
リソースアクセスコントロール部に
メッセージを送信
55
情報伝達部にメッセージを送信
56

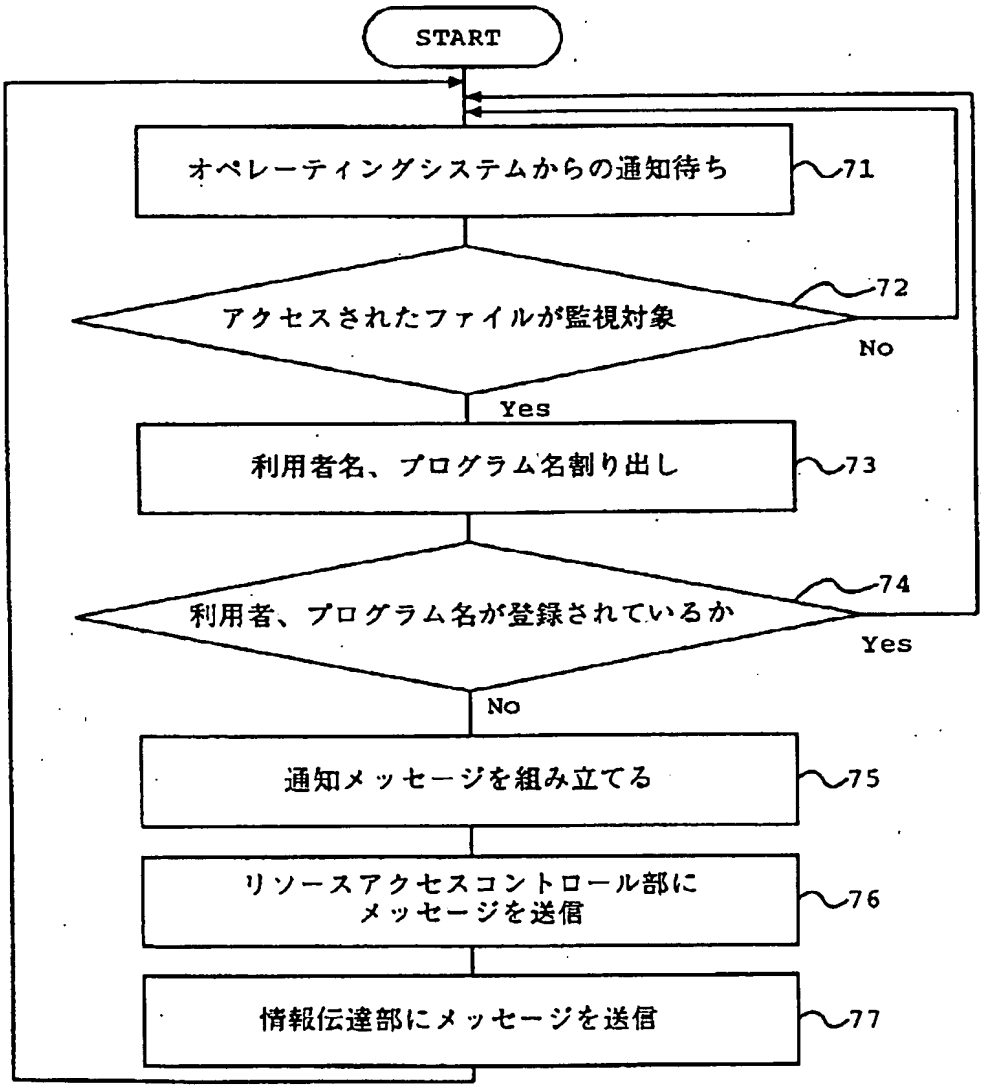
【図6】

図 6


START
パケット送受信数を取得
61
取得パケット数 > 内部状態定義テーブル記述内容
62
Yes
No
一定時間スリープ
63
通知メッセージを組み立てる
64
リソースアクセスコントロール部に
メッセージを送信
65
情報伝達部にメッセージを送信
66

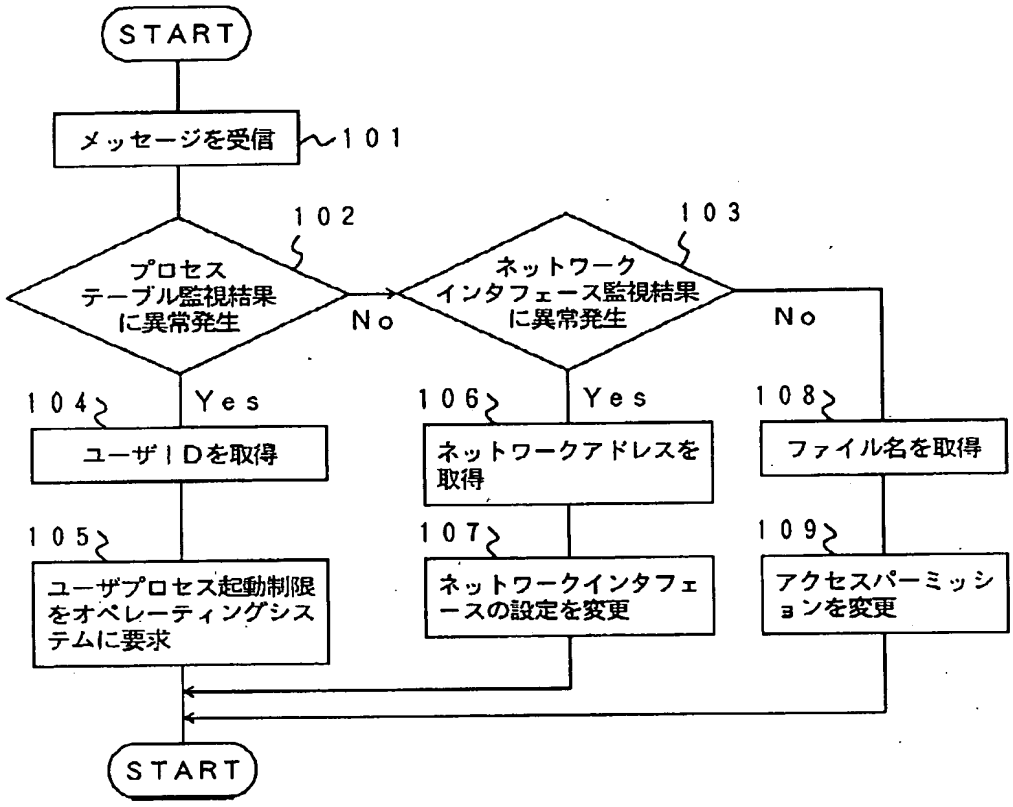
【図7】

図 7


START
オペレーティングシステムからの通知待ち
71
アクセスされたファイルが監視対象
72
No
Yes
利用者名、プログラム名割り出し
73
利用者、プログラム名が登録されているか
74
Yes
No
通知メッセージを組み立てる
75
リソースアクセスコントロール部に
メッセージを送信
76
情報伝達部にメッセージを送信
77

【図１０】

図１０


START
メッセージを受信
１０１
１０２
プロセス
テーブル監視結果
に異常発生
No
１０３
ネットワーク
インタフェース監視結果
に異常発生
No
１０４
Yes
ユーザＩＤを取得
１０５
ユーザプロセス起動制限
をオペレーティングシス
テムに要求
１０６
Yes
ネットワークアドレスを
取得
１０７
ネットワークインタフェ
ースの設定を変更
１０８
ファイル名を取得
１０９
アクセスパーミッシ
ョンを変更
START